REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks.

By this amendment, claims 1, 12 and 19 are amended. No new matter has been added. Accordingly, claims 1-10 and 12-19 are pending in the present application.

Claim Objection

Claims 1, 12 and 19 are objected to on the basis of informalities.

The foregoing amendments to claims 1, 12 and 19 address each of the Examiner's concerns. Accordingly, it is respectfully requested that the objection to claims 1, 12 and 19 be withdrawn.

Claim Rejections Under 35 U.S.C. § 101

Claims 1-10 and 16-18 are rejected under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter.

Applicants respectfully disagree with the assertion that the steps recited in the claimed methods can be completely performed mentally, verbally, or without a machine. For example, claim 1 clear recites "storing the pairs or values thus obtained in a memory of a secure electronic object." Accordingly, the method recited in claim 1 is at least tied to a particular machine, e.g., the secure electronic object.

However, to expedite prosecution of the present application, Applicants have amended claim 1, for clarification, to recite "obtaining values for e and l by the secure electronic object," and "verifying, by the secure electronic object, the following

conditions for said pair of prime numbers..." As such, the method recited in claim 1 cannot be completely performed mentally, verbally, or without a machine.

In view of the foregoing, it is respectfully requested that the rejection of claims 1-10 and 16-18 under 35 U.S.C. §101 be withdrawn.

Claim Rejection Under 35 U.S.C. § 103

Claims 1-5, 12, 13, 15, 16 and 19 are rejected under 35 U.S.C. §102(e) as allegedly being unpatentable over Hopkins et al. (U.S. Patent Application Publication No. 2005/0190912 A1, hereinafter "Hopkins") in view of Hopkins et al. (U.S. Patent Application Publication No. 2002/0186837, referred to in the Office Action as "Hopkins914"). The rejection is respectfully traversed.

Applicants' exemplary embodiments relate to a method of generating electronic keys d for a public-key cryptography method using a secure electronic device, the method comprising two separate calculation steps:

Step A

- 1) calculating pairs of prime numbers (p,q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of the pair (e,l) in which e is the public exponent and l is the length of the key of the cryptography method, l also being the length of the modulus N of said method,
- 2) storing the pairs or values thus obtained in the memory of the secure electronic device; and

Step B

- calculating the key d to be used by secure electronic device from the results of step A and knowledge of the pair (e,l).

According to Applicants' exemplary embodiments, the calculation steps A and B are separate in terms of time. Step A, which corresponds to a relatively complex calculation compared to Step B, may be carried out by an element other than the secure electronic device, for example by a server. In this case, the results of the calculation of this first step may be loaded onto a chip card during personalization. The calculation of step A may also be carried out by the card itself at any given instant which does not disturb the user of this card. For example, this calculation may be carried out during personalization of the card or subsequently.

Claim 1 recites a method of generating electronic keys d for a public-key cryptography method using a secure electronic device, comprising the following two separate calculation steps:

Step A

1) ...

2) storing the calculated pairs of prime numbers or values in a memory of the secure electronic object; and

Step B

...

in response to the secure electronic object being requested to generate a private key, retrieving a pair of prime numbers (p, q), or a value representative of said pair of prime numbers, stored in Step A;

... ; and

calculating a key d to be used by the secure electronic object from the retrieved pair (p, q) that is determined to be suitable.

Hopkins and Hopkins914, whether considered individually or in combination, do not disclose the above recited features of claim 1. Hopkins discloses providing cryptographic parameters by a server for use in cryptographic applications in response to requests. Referring to Fig. 2 of Hopkins, the server system 32 pre-computes and securely stores a plurality of different types of sets of cryptographic parameters to be used by applications residing on remote clients 34. In paragraphs 0087 and 0088, Hopkins, describes that each type of set is adapted for use by an associated type of cryptographic application. Each application may use a modulus n having different length L and may employ a different public exponent e. For this reason, therefore, "[e]ach type of set of cryptographic parameters includes...an associated length L and ...an associated public key exponent value e..." By means of this arrangement, when the server 32 receives a request for cryptographic parameters for a specific application, it is able to service the request with a set of parameters that meet the length and public exponent requirements of that application with minimal latency (paragraph 0090).

According to claim 1, pairs of prime numbers (p, q) or values representative of pairs of prime numbers calculated in Step A are stored in a memory of the secure electronic object. A key d based on a pair of prime numbers (p, q) or values selected from the pairs of prime numbers (p, q) or values stored in the secure electronic object is calculated and used by the secure electronic object. Hopkins does not disclose a method that includes storing calculated pairs of prime numbers or values in a memory of the secure electronic object, and then calculating a key d to be used by the secure electronic object from the retrieved pair (p, q) that is determined to be suitable, as recited in claim 1. Rather, in Hopkins, the prime numbers are stored in the server 32, and the private key exponent d is determined in the server 32.

However, the server 32 does not use that key, e.g. for a cryptographic operation. Rather, the private key exponent value d is included in the set of cryptographic parameters that are provided from the server 32 to the client 34 (paragraph 0087). It is the client 34 that uses the key for a cryptographic operation. The prime numbers are not stored in the client, nor does the client calculate the key d from such prime numbers. As such, Hopkins does not meet the language of the claims.

In addition, claim 1 recites a method comprising "prior to the secure electronic object receiving a request to generate a private key, calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of a pair of values (e, l) in which e is the public exponent and l is the length of the key of the cryptography method."

Hopkins does not disclose the above-recited features of claim 1. Fig. 6 of Hopkins illustrates a process of providing pre-computed cryptographic parameters of different types. As noted previously, the pre-computed cryptographic parameters are generated for different values of length L and public exponent e. Consequently, the individual computation must be performed with a priori knowledge of these values. In contrast, according to claim 1, pairs of prime numbers (p, q) or values representative of pairs of prime numbers, which are stored in the memory of the electronic object, are calculated independent of knowledge of a pair of values (e, l). Consequently, Hopkins fails to disclose the above-recited features of claim 1.

In rejecting claim 1, the Office Action alleges that Hopkins discloses calculating pairs of prime numbers independent of knowledge of a pair of values for e and l, with reference to paragraph 0038. However, Applicants are unable to identify any support for this assertion. In fact, when read in light of paragraphs 0087, 0088 and 0090, discussed above, the cited paragraph suggests just the

opposite. The ability to respond to a request for a prime number value having a specified length with minimal latency can only be achieved if the value for that length is know a priori and associated with a specific prime number, or set of prime numbers.

If the rejection is not withdrawn, the Examiner is requested to explain, with particularity, how Hopkins is being interpreted to disclose calculation of prime numbers "independent of knowledge of a pair of values for 3 and l." In the absence of such a showing, it is respectfully submitted that the rejection is unsupported.

In claim 1, Step A comprises the calculation of pairs of prime numbers independently of the knowledge of values for the public exponent and the length, and storage of these prime number pairs in memory of the secure electronic object. Because the pairs of prime numbers are not associated with specific values for the public exponent and the length when they are stored, Step B is carried out once specific values for these two parameters are obtained by the secure electronic object. Specifically, when a request is made to generate a private key corresponding to those specific values, a determination must be made whether a given pair of prime numbers retrieved from the memory correspond to those values. It is for this purpose that the verification process of Step B is carried out.

In contrast, in Hopkins the prime numbers are already associated with specific values for the public exponent and the modulus length. As such, there is no need to perform such a verification process when providing the cryptographic parameters to the client 34. Consequently, Hopkins does not disclose the claimed verification, as acknowledged in the Office Action.

Hopkins914 is relied upon as allegedly disclosing the verification of a pair of prime numbers. Applicants respectfully submit that Hopkins914 does not disclose

the specific type of verification recited in claim 1. However, even if it could be interpreted to disclose such, there is no reason to employ such verification in the context of Hopkins. As noted above, in Hopkins the prime numbers are associated with specific values for e and I. Consequently, there is no reason to verify whether a particular pair of numbers meet the criteria set forth in claim 1. That determination has already been made.

In summary, the references do not disclose calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers independent of knowledge of a pair of values (e, I), storing the calculated pairs of prime numbers or values in the secure electronic object, or that a key calculated based on one of the stored pairs is used by the secure electronic object, as described in claim 1.

At least for the reasons above, claim 1 is patentable. Independent claims 12 and 19 are patentable at least because they include distinguishing features similar to those of claim 1. Claims 2-5, 13, 15 and 16 are patentable at least because of their dependency.

Claims 6, 8-10, 14, 17 and 18 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hopkins and Hopkins914, as applied to claims 1, 3, 5 and 13, and further in view of Futa et al. (U.S. Patent No. 7,130,422 B2, hereinafter "Futa").

Futa discloses a method of generating a prime N after receiving an input of prime q, wherein N is larger than q. Futa does not remedy the above-mentioned deficiencies of Hopkins and Hopkins914. Therefore, claims 6, 8-10, 14, 17 and 18 are patentable.

Claim 7 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hopkins and Hopkins914, and further in view of Matyas (U.S. Patent No. 4,736,423, hereinafter "Matyas").

Matyas relates to reducing the size of cryptographic keys for storage on magnetic strip cards. Matyas does not remedy the above-mentioned deficiencies of Hopkins and Hopkins914. Therefore, claim 7 is patentable.

CONCLUSION

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: December 23, 2010

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839
703 836 6620